CALL FOR PAPERS

6th International Conference on Applied Cryptography and Network Security (ACNS '08), June 3-6, 2008, Columbia University, New York, NY, USA

Submissions due: January 14, 2008
Notification by: March 14, 2008

http://acns2008.cs.columbia.edu/

General Chair
Angelos Keromytis (Columbia University, USA)
Moti Yung (Google Inc., USA)

Program Chairs
Steven Bellovin (Columbia University, USA)
Rosario Gennaro (IBM Research, USA)

Publicity Chair
Jianying Zhou (I^2R, Singapore)

Program Committee
Masayuki Abe (NTT, Japan)
Ben Adida (Harvard University, USA)
Feng Bao (I^2R, Singapore)
Lujo Bauer (Carnegie Mellon University, USA)
Giampaolo Bella (University of Catania, Italy)
Steven Bellovin, co-chair (Columbia University, USA)
John Black (University of Colorado, USA)
Nikita Borisov (U. of Illinois Urbana-Champaign, USA)
Colin Boyd (Queensland U. of Technology, Australia)
Dario Catalano (University of Catania, Italy)
Debra Cook (Alcatel-Lucent Bell Labs, USA)
Alexander W. Dent (Royal Holloway, U. of London, UK)
Nelly Fazio (IBM Research, USA)
Marc Fischlin (Darmstadt U. of Technology, Germany)
Debin Gao (Singapore Management U., Singapore)
Rosario Gennaro, co-chair (IBM Research, USA)
Peter Gutmann (University of Auckland, New Zealand)
Moses Liskov (William & Mary College, USA)
John Ioannidis (Packet General Networks, USA)
Stanislaw Jarecki (University of California Irvine, USA)
Ari Juels (RSA Laboratories, USA)
Kaoru Kurosawa (Ibaraki University, Japan)
Yehuda Lindell (Bar-Ilan University, Israel)
Javier Lopez (University of Malaga, Spain)
Jelena Mirkovic (USC/ISI, USA)
David Naccache (Ecole Normale Supérieure, France)
Alina Oprea (RSA Laboratories, USA)
Tom Shrimpton (Portland State University, USA)
Jonathan Smith (University of Pennsylvania, USA)
Angelos Stavrou (George Mason University, USA)
Xiaoyun Wang (Shandong University, China)
Nicholas Weaver (ICSI Berkeley, USA)
Steve Weis (Google Inc., USA)
Tara Whalen (Dalhousie University, Canada)
Michael Wiener (Cryptographic Clarity, Canada)
Avishai Wool (Tel-Aviv University, Israel)
Diego Zamboni (IBM Research, Switzerland)
Jianying Zhou (I^2R, Singapore)

Original papers on all aspects of applied cryptography and network security are solicited for submission to ACNS '08. Topics of relevance include but are not limited to:

- Applied cryptography and provably-secure cryptographic protocols
- Design and analysis of efficient cryptographic primitives: public-key and symmetric-key cryptosystems, block ciphers, and hash functions
- Network security protocols
- Techniques for anonymity; trade-offs between anonymity and utility
- Integrating security into the next-generation Internet: DNS security, routing, naming, denial-of-service attacks, TCP/IP, secure multicast
- Economic fraud on the Internet: phishing, pharming, spam, and click fraud
- Email and web security
- Public key infrastructure, key management, certification, and revocation
- Security and privacy for emerging technologies: sensor networks, mobile (ad hoc) networks, peer-to-peer networks, bluetooth, 802.11, RFID
- Trust metrics and robust trust inference in distributed systems
- Security and usability
- Intellectual property protection: metering, watermarking, and digital rights management
- Modeling and protocol design for rational and malicious adversaries
- Automated analysis of protocols

Papers suggesting novel paradigms, original directions, or non-traditional perspectives are especially welcome.

As in previous years, there will be an academic track and an industrial track. Submissions to the academic track should emphasize research contributions, while submissions to the industrial track may focus on implementation and deployment of real-world systems. Submissions for the industrial track must clearly indicate this in the title. Proceedings for the academic track will be published in Springer-Verlag's Lecture Notes in Computer Science and will be available at the conference. Papers accepted to the industrial track will be published in a different venue.

Instructions for authors: Submissions must be anonymous, with no author names, affiliations, acknowledgments, or obvious references. Submissions should be in English, in PDF format with all fonts embedded, typeset with 11pt font or larger, and using reasonable spacing and margins. They should not exceed 12 letter-sized pages, not counting the bibliography and appendices. Papers should begin with a title, abstract, and an introduction that clearly summarizes the contributions of the paper at a level appropriate for a non-specialist reader. Papers should contain a scholarly exposition of ideas, techniques, and results, including motivation, relevance to practical applications, and a clear comparison with related work. Committee members are not required to read appendices, and papers should be intelligible without them. Submitted papers risk being rejected without consideration of their merits if they do not follow all the above guidelines.

Submissions must not substantially duplicate work that was published elsewhere, or work that any of the authors has submitted in parallel to any other conference or workshop that has proceedings. **Plagiarism** and **double submissions** will be dealt with harshly.

Authors will be asked to indicate whether their submissions should be considered for the best student paper award; any paper co-authored by a full-time student is eligible for this award.

Authors of accepted papers must guarantee that their paper will be presented at the conference.

Submission Website https://s1.iacr.org/websubrev/acns2008/submit/